Amazon One Payment Study

Identification: Aditya Iyer and Kenneth James Wall (Group 5)

Abstract:

This report examines user trust in Amazon One, a biometric palm-payment system, using the Human-Computer Trust Scale (HCTS). A survey of 22 participants revealed moderate trust levels, while users found the system technically competent, concerns about privacy, data handling, and regulatory safeguards were significant. Trust varied by age, gender, and tech familiarity. The report highlights key adoption barriers and offers recommendations for building trust through better transparency, privacy protections, and user-centered design.

Introduction:

Biometric payment technologies are becoming increasingly integrated into everyday retail and digital transactions. Among them, Amazon One represents an approach using palm recognition as a method of identity verification and payment. As this technology continues to expand in public spaces, understanding how it is perceived by users becomes critical for guiding its ethical development and acceptance.

This report presents findings from a user perception study of Amazon One. The goal is to explore users' trust, privacy concerns, and willingness to adopt biometric payment systems for everyday transactions. It also investigates how demographic factors such as age, technology familiarity, and privacy sensitivity affect the perceived risks and benefits of the system.

The Object of Evaluation:

The Goal of the Study

The primary goal of this study is to examine how users perceive and respond to Amazon One, a biometric payment system that uses palm recognition for transactions. The study aims to evaluate user trust, privacy concerns, and willingness to adopt the system in everyday retail settings. It also investigates how different demographic and social groups interpret the **risks and benefits** associated with this technology.

The study seeks to:

- To explore **users' trust in biometric payment systems** and their **willingness to adopt Amazon One** for everyday transactions.
- To investigate **how privacy concerns** influence users' acceptance of Amazon One.

- To analyze how different **demographic and social groups** (age, tech familiarity, privacy awareness) perceive the risks and benefits of Amazon One.

The Problem:

The use of biometric data in consumer technologies raises **ethical, social, and privacy concerns**. While biometric systems offer convenience and security, they also introduce new risks related to **surveillance, data misuse, and a lack of user control**. Amazon One, being a palm-based biometric system, further complicates this by introducing **a new and unfamiliar method of authentication**, which may cause hesitation among users.

With an increasing deployment of biometric payment solutions, there remains a **knowledge gap** in how people from various backgrounds perceive these technologies. There is also limited public understanding of **how biometric data is stored, shared, and protected**. Without clear insight into user concerns, adoption of such technologies may get stalled or proceed without adequate safeguards in place.

How Amazon One is Human-Like Technology:

- It interacts with the user's physical body (the palm) rather than an abstract identifier like a password or card.
- The technology tailors access to a unique individual, simulating a form of human recognition.
- It operates independently and initiates secure transactions without manual intervention.

Why Trust Is Critical in These Scenarios:

As technologies become more human-like, the stakes of trust increase. Users need to delegate tasks, such as payment or personal data management, to systems they may not fully understand. Without trust, adoption falters even if the technology is technically secure or efficient.

Procedure:

A survey was designed and conducted online to collect participant perspectives after introducing them to the system through a short orientation video.

The steps in the procedure were:

- Participants were invited via personal networks.
- An official Amazon One demo video was embedded directly into the Google Form to provide all participants with a uniform introduction to the technology.
- Respondents completed a structured questionnaire.
- All responses were collected via Google Forms and stored in Google Sheets.
- Responses were analyzed using cross-tabulations and comparisons across demographic and social variables.

Apparatus and Materials:

- **Orientation Material:** Embedded YouTube video – Amazon One Demo
- **Survey Platform:** Google Forms
- **Data Storage and Analysis Tool:** Google Sheets
- **Trust Measurement Framework:** Human-Computer Trust Scale (HCTS), used to assess constructs like risk perception, benevolence and competence.

Method - Questionnaire Design:

- **Section 1:** Demographics (age, gender, occupation, tech experience, privacy sensitivity, shopping preferences).
- **Section 2:** Likert-scale statements measuring risk perception, benevolence, competence and the overall trust.
- **Section 3:** Open-ended questions exploring concerns, suggestions, and openness to using Amazon One or other biometric alternatives.

Participants

- **Total Respondents**: 22
- **Gender**:
    - **Male:** 15
    - **Female:** 7

Age Groups:

- **18–30 years:** 16
- **31–45 years:** 5
- **46+ years:** 1

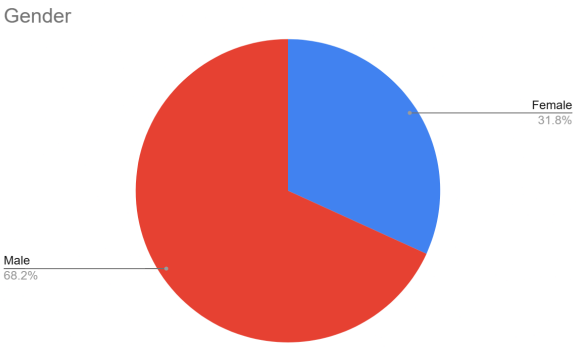

Figure 1: Gender

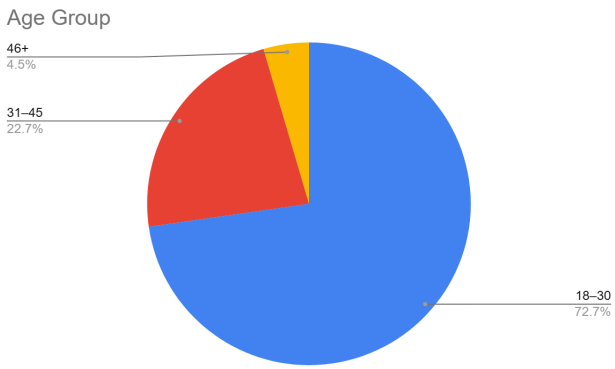

Figure 2: Age Group

Results and Discussion

This study employed the **Human-Computer Trust Scale (HCTS)** to measure user trust across three key dimensions:

- **Risk Perception:** If users think a system might cause harm or mistakes, they will trust it less.
- **Benevolence:** If users feel the system is designed to help them and act in their best interest, they will trust it more.
- **Competence:** If the system works well and does what it promises, users trust it more.

Each dimension was measured using a set of Likert-scale items, and overall trust was assessed with a separate direct rating.

Reliability: Cronbach's Alpha

To ensure the internal consistency of the instrument, Cronbach's Alpha was calculated across trust-related items. The result, **α = 0.71**, indicates **acceptable reliability**, suggesting that the instrument measured the intended constructs consistently across participants.

Descriptive Statistics and Key Patterns

Overall Trust Levels

The average trust level across all 22 participants was **64.92%**, indicating moderate but cautious trust in Amazon One as a biometric payment system. Trust is not uniformly distributed across demographics:

- **By Gender:**
  - **Males** reported a **slightly higher trust level (66.33%)** than **females (61.90%)**, consistent with broader findings that privacy-aware users (more common among females in this study) show greater hesitation.
- **By Age Group:**
  - Trust generally increases **slightly with age**:
    - **18–30 years: 64.17%**
    - **31–45 years: 66.67%**
    - **46+ years: 68.33%**
- Despite a small sample in the 46+ category, the data suggests that older users may perceive Amazon One as more trustworthy, possibly due to familiarity with institutional systems or lower concern over emerging data practices.

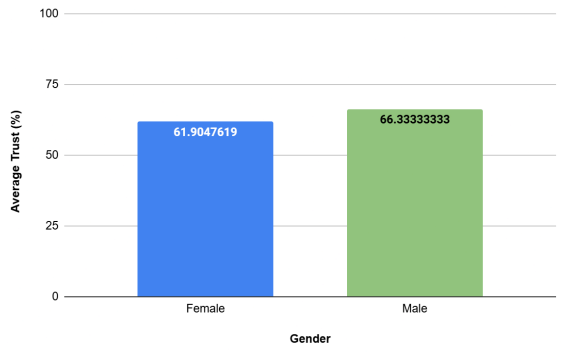

Figure 3: Trust Percentage by Gender

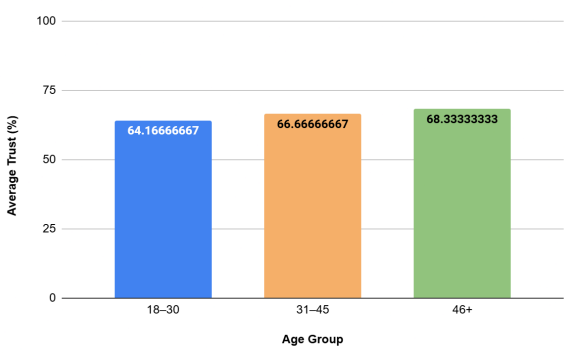

Figure 4: Trust Percentage by Age Group

Trust Dimensions

- **Risk Perception** (Mean: 3.12): Users expressed neutral-to-slight concern, indicating they are cautious but not overtly alarmed.
- **Benevolence** (Mean: 3.48): Users were mildly positive, suggesting they believe Amazon One may have good intentions, but aren't fully convinced.
- **Competence** (Mean: 3.87): This was the highest-rated factor, indicating strong confidence in Amazon One's technical performance.

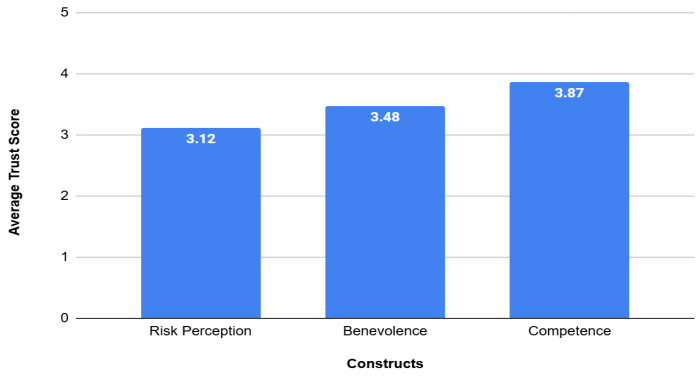

Figure 4: Mean values for the HCTS Constructs

Insights from Responses

- **Data Security (72.7%)** and **Privacy (59.1%)** were cited as the top concerns across groups.
- Participants frequently asked for **clear privacy policies**, the **ability to delete biometric data**, and **PIN backups** as fallback options.
- Some users mentioned **distrust in Amazon as a company**, highlighting broader brand-related skepticism.
- **Health concerns**, such as shared surfaces and hygiene (18.2%), were mentioned but not dominant.

Demographic Insights

- **Younger males and tech-savvy users** were generally more trusting and open to using Amazon One.
- **Female participants** and those with **high privacy sensitivity** were more cautious, particularly around data storage and legal safeguards.

Adoption and Biometric Openness

- **38.1%** of users said they would use **Amazon One frequently**.
- However, **52.4%** expressed hesitancy, saying they might adopt it but only with additional guarantees (e.g., transparent policies, optional PINs).
- Openness to other biometric methods:
    - **38.1%** were open to using alternatives like facial or fingerprint recognition.
    - **28.6%** were uncertain.

- **33.3%** were not open to biometric methods at all, typically due to privacy or control concerns.

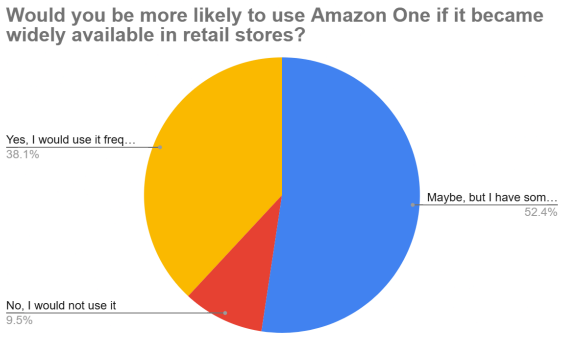
Would you be more likely to use Amazon One if it became widely available in retail stores?
Yes, I would use it freq...
38.1%
Maybe, but I have som...
52.4%
No, I would not use it
9.5%

Figure 5: Willingness to Use Amazon One

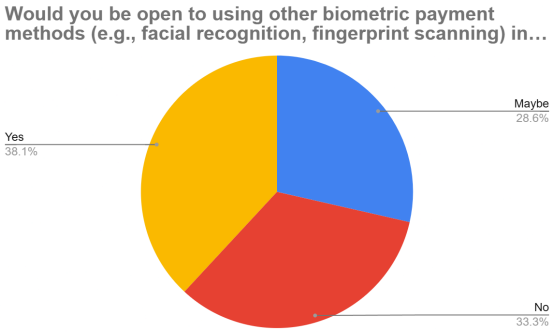

Figure 6: Open to Use Other Biometric Systems

Overall Discussion

These findings show us there is a measured optimism and cautious trust toward Amazon One. While users are largely confident in the system's technical competence, they are wary of how their biometric data is managed and protected. The gap between trust in performance and trust in ethical/legal handling of personal information is vital to the adoption challenge.

If Amazon One or similar technologies aim to achieve broad adoption, they must go beyond functionality and address users' emotional and ethical expectations. Transparency, regulation, and user control must become the core features.

Issues to Address and Recommendations:

Overall, users are not yet ready to fully trust Amazon One. The most significant trust barriers identified in the study include:

- **Data Security and Privacy Concerns:** A majority of users (72.7% and 59.1%, respectively) expressed deep concerns about the security of their biometric data and how it may be used, stored, or shared.
- **Lack of Transparency:** Trust in Amazon's data handling practices was low, indicating that users feel uninformed and uneasy about what happens to their data after collection.
- **Weak Regulatory Confidence:** Confidence in legal and regulatory safeguards was modest, suggesting users are unsure if adequate protections are enforced.
- **Absence of Backup Authentication:** The lack of alternative login options, such as PINs or passwords, was seen as a vulnerability that increases user hesitation.
- **Distrust in Amazon's Intentions:** Only a small share (36.4%) expressed trust in Amazon as a brand, indicating that broader perceptions of the company negatively affect willingness to adopt its biometric system.

- **Demographic Trust Gaps:** Younger, tech-savvy males showed relatively higher levels of trust, while females and privacy-conscious individuals were notably more skeptical. This highlights the importance of audience-specific trust-building strategies.
- **Secondary but Notable Concerns:** Hygiene-related fears and health risks, although mentioned by fewer users (18.2%), remain relevant for a system involving physical contact.

To increase adoption and build trust, Amazon One should focus on:

- **Strengthening data protection measures:** Implement advanced security protocols and regularly audit systems to reassure users that their biometric data is safe from breaches or misuse.
- **Enhancing transparency and user education:** Communicate how biometric data is collected, stored, and used. Provide users with accessible privacy policies and real-world examples to foster informed consent.
- **Supporting regulatory clarity:** Advocate for and comply with clear legal frameworks around biometric data usage to reinforce public confidence and demonstrate accountability.
- **Offering hybrid authentication methods:** Give users alternatives such as PINs or mobile verification to provide a sense of control and reduce reliance on a single biometric method.
- **Proactively addressing brand trust and ethical concerns:** Acknowledge concerns about corporate motives and commit to ethical data practices, reinforcing Amazon's role as a responsible innovator.

Study Reflections

During the implementation phase, we faced challenges related to participant recruitment and study planning. Our respondent pool was skewed:

- **Regionally limited**, which may obscure how cultural attitudes toward privacy and biometric tech affect trust.
- **Age-biased**, with a dominance of younger users, who may be more familiar with technology but less reflective of broader societal concerns.
- **Gender-skewed**, with more male than female respondents, despite evidence that privacy sensitivity differs by gender.

These imbalances limited the generalizability of our findings and likely affected the quality of our data. A more strategic sampling approach and earlier recruitment planning would have produced more reliable demographic representation.

Conclusion:

The study shows that although Amazon One is seen as competent with a moderate trust level of **64.92%**, it is hindered by privacy and transparency concerns. Younger, tech-savvy users are more open to adoption, while privacy-sensitive users remain cautious. Key trust barriers include

unclear data practices, weak legal confidence, and lack of alternative authentication. To build trust in such human-like technologies, companies must prioritize transparency, privacy, and inclusive design strategies.